MRD CODES WITH MAXIMUM IDEALISERS

BENCE CSAJBÓK [1], GIUSEPPE MARINO [2,3], OLGA POLVERINO [3], AND YUE ZHOU [4]

Abstract. Left and right idealizers are important invariants of linear rank-distance codes. In the case of maximum rank-distance (MRD for short) codes in $\mathbb{F}_q^{n\times n}$ the idealizers have been proved to be isomorphic to finite fields of size at most q^n. Up to now, the only known MRD codes with maximum left and right idealizers are generalized Gabidulin codes, which were first constructed in 1978 by Delsarte and later generalized by Kshevetskiy and Gabidulin in 2005. In this paper we classify MRD codes in $\mathbb{F}_q^{n\times n}$ for $n \leq 9$ with maximum left and right idealizers and connect them to Moore-type matrices. Apart from generalized Gabidulin codes, it turns out that there is a further family of rank-distance codes providing MRD ones with maximum idealizers for $n = 7$, q odd and for $n = 8$, $q \equiv 1 \pmod 3$. These codes are not equivalent to any previously known MRD code. Moreover, we show that this family of rank-distance codes does not provide any further examples for $n \geq 9$.

1. Introduction

For two positive integers m and n and for a field $\mathbb{K}$, let $\mathbb{K}^{m\times n}$ denote the set of all $m \times n$ matrices over $\mathbb{K}$. The *rank metric* or the *rank distance* on $\mathbb{K}^{m\times n}$ is defined by

$$d(A, B) = \operatorname{rank}(A - B),$$

for any $A, B \in \mathbb{K}^{m\times n}$.

A subset $\mathcal{C} \subseteq \mathbb{K}^{m\times n}$ with respect to the rank metric is usually called a *rank-metric code* or a *rank-distance code*. When $\mathcal{C}$ contains at least two elements, the *minimum distance* of $\mathcal{C}$ is given by

$$d(\mathcal{C}) = \min_{A,B\in\mathcal{C},A\neq B}\{d(A, B)\}.$$

When $\mathcal{C}$ is a $\mathbb{K}$-linear subspace of $\mathbb{K}^{m\times n}$, we say that $\mathcal{C}$ is a $\mathbb{K}$-linear code and its dimension $\dim_{\mathbb{K}}(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{K}$.

Let $\mathbb{F}_q$ denote the finite field of q elements. For any $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with $d(\mathcal{C}) = d$, it is well-known that

$$\#\mathcal{C} \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)},$$

which is a Singleton like bound for the rank metric; see [13]. When equality holds, we call $\mathcal{C}$ a *maximum rank-distance* (MRD for short) code. More properties of MRD codes can be found in [13], [18], [20], [40] and [45].

The research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) and by the project "VALERE: VAnviteLli pEr la RicErca" of the University of Campania "Luigi Vanvitelli". The first author is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and partially by OTKA Grant No. PD 132463 and OTKA Grant No. K 124950. The fourth author is supported by the National Natural Science Foundation of China (No. 11771451).

Rank-metric codes, in particular MRD codes, have been studied since the 1970s and have seen much interest in recent years due to a wide range of applications including storage systems [46], cryptosystems [19], spacetime codes [36] and random linear network coding [28].

In finite geometry, there are several interesting structures, including quasifields, semifields, splitting dimensional dual hyperovals and maximum scattered subspaces, which can be equivalently described as special types of rank-distance codes; see [8], [14], [15], [48], [51] and the references therein. In particular, a finite quasifield corresponds to an MRD code in $\mathbb{F}_q^{n\times n}$ of minimum distance n and a finite semifield corresponds to an MRD code that is a subgroup of $\mathbb{F}_q^{n\times n}$ (see [12] for the precise relationship). Many essentially different families of finite quasifields and semifields are known [27], [30], which yield many inequivalent MRD codes in $\mathbb{F}_q^{n\times n}$ of minimum distance n.

There are several slightly different definitions of equivalence of rank-distance codes. In this paper, we use the following notion of equivalence.

Two rank-distance codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{K}^{m\times n}$ are *equivalent* if there exist $A \in \mathrm{GL}_m(\mathbb{K})$, $B \in \mathrm{GL}_n(\mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\rho \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AM^\rho B + C \colon M \in \mathcal{C}_1\}. \tag{1}$$

The *adjoint code* of a rank-metric code $\mathcal{C}$ in $\mathbb{K}^{m\times n}$ is

$$\mathcal{C}^\top := \{M^T \in \mathbb{K}^{n\times m} \colon M \in \mathcal{C}\},$$

where $(\,.\,)^T$ denotes transposition. If $\mathcal{C}$ is a linear MRD code then $\mathcal{C}^\top$ is also a linear MRD code. For $m = n$, if $\mathcal{C}_2$ is equivalent to $\mathcal{C}_1$ or $\mathcal{C}_1^\top$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are called *isometrically equivalent*. An equivalence map from a rank-distance code $\mathcal{C}$ to itself is also called an *automorphism* of $\mathcal{C}$.

When $\mathcal{C}_1$ and $\mathcal{C}_2$ are both additive and equivalent, it is not difficult to show that we can choose $C = 0$ in (1).

In general, it is a difficult job to tell whether two given rank-distance codes are equivalent or not. There are several invariants which may help us distinguish them. Given a $\mathbb{K}$-linear rank-distance code $\mathcal{C} \subseteq \mathbb{K}^{m\times n}$, following [32] its *left* and *right idealisers* are defined as

$$L(\mathcal{C}) = \{M \in \mathbb{K}^{m\times n} \colon MC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

and

$$R(\mathcal{C}) = \{M \in \mathbb{K}^{m\times n} \colon CM \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

respectively. The left and right idealisers can be viewed as a natural generalization of the middle and right nucleus of semifields [35] and some authors call them in this way. In general, we can also define the left nucleus of $\mathcal{C}$ which is another invariant for semifields. However, for MRD codes in $\mathbb{F}_q^{m\times n}$ with minimum distance less than $\min\{m, n\}$, the left nucleus is always $\mathbb{F}_q$ which means that it is not a useful invariant; see [35].

The *Delsarte dual code* of an $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is

$$\mathcal{C}^\perp := \{M \in \mathbb{F}_q^{m\times n} \colon \mathrm{Tr}(MN^T) = 0 \text{ for all } N \in \mathcal{C}\}.$$

If $\mathcal{C}$ is a linear MRD code then $\mathcal{C}^\perp$ is also a linear MRD code as it was proved by Delsarte [13].

Two MRD codes in $\mathbb{F}_q^{n\times n}$ with minimum distance n are equivalent if and only if the corresponding semifields are isotopic [30, Theorem 7]. In contrast, it appears to

be much more difficult to obtain inequivalent MRD codes in $\mathbb{F}_q^{n\times n}$ with minimum distance strictly less than n. We divide the known constructions of inequivalent MRD codes in $\mathbb{F}_q^{n\times n}$ of minimum distance strictly less than n into two types.

(1) The first type of constructions consists of MRD codes of minimum distance d for arbitrary $2 \le d \le n$.
   - The first construction of MRD codes which was given by Delsarte [13] and later rediscovered by Gabidulin [18] and generalized by Kshevetskiy and Gabidulin [29]. They are usually called the (generalized) Gabidulin codes. In 2016, Sheekey [48] found the so-called (generalized) twisted Gabidulin codes. They can be generalized into additive MRD codes [43]. Very recently, by using skew polynomial rings Sheekey [49] proved that they can be further generalized into a quite big family and all the MRD codes mentioned above can be obtained in this way.
   - The non-additive family constructed by Otal and Özbudak in [44].
   - The family appeared in [52] which is related to the Hughes-Kleinfeld semifields.

(2) The second type of constructions provides us MRD codes of minimum distance $d = n - 1$.
   - Non-linear MRD codes by Cossidente, the second author and Pavese [5] which were later generalized by Durante and Siciliano [17].
   - Linear MRD codes associated with maximum scattered linear sets of $\mathrm{PG}(1, q^6)$ and $\mathrm{PG}(1, q^8)$ presented recently in [1, 7, 9, 38, 54].

For the relationship between MRD codes and other geometric objects such as linear sets and Segre varieties, we refer to [33]. For more results concerning maximum scattered linear sets and associated MRD codes, see [2], [6], [8], [10], [11] and [50].

Compared to the known MRD codes in $\mathbb{F}_q^{n\times n}$ listed above, there are slightly more ways to get MRD codes in $\mathbb{F}_q^{m\times n}$ with $m < n$, see [8], [16], [25], [42] and [47].

For an MRD code $\mathcal{C}$ in $\mathbb{F}_q^{n\times n}$, by [35, Corollary 5.6], its left and right idealisers are isomorphic to finite fields of size at most q^n. Moreover, according to [35, Proposition 4.2] if the left and right idealisers of an MRD code $\mathcal{C}$ in $\mathbb{F}_q^{n\times n}$ are both isomorphic to $\mathbb{F}_{q^n}$, then the same holds for $\mathcal{C}^\top$ and $\mathcal{C}^\perp$.

Among the $\mathbb{F}_q$-linear MRD codes listed in (1) and (2), only the generalized Gabidulin codes have this special property. Thus, it is natural to ask whether there exist other MRD codes in $\mathbb{F}_q^{n\times n}$ with maximum left and right idealisers. In this paper, we classify $\mathbb{F}_q$-linear MRD codes $\mathcal{C}$ in $\mathbb{F}_q^{n\times n}$, $n \le 9$, with $L(\mathcal{C}) \cong R(\mathcal{C}) \cong \mathbb{F}_{q^n}$ up to the adjoint and Delsarte dual operations. In particular, our classification includes new examples of such MRD codes for $n = 7$, q odd (cf. Theorem 3.3 and Corollary 3.4), and for $n = 8$, $q \equiv 1 \pmod 3$ (cf. Theorem 3.5 and Corollary 3.6).

More precisely, we prove the following result.

Theorem 1.1. *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MRD code in $\mathbb{F}_q^{n\times n}$ with left and right idealisers isomorphic to $\mathbb{F}_{q^n}$, $n \ge 2$.*

- *If $n \le 6$ or $n = 9$ then $\mathcal{C}$ is equivalent to a generalized Gabidulin code.*
- *If $n = 7$ then $\mathcal{C}$ is equivalent to a generalized Gabidulin code or q is odd and, up to the adjoint operation, $\mathcal{C}$ is equivalent either to*

$$\mathcal{C}_7 := \{a_0X + a_1X^q + a_2X^{q^3} : a_0, a_1, a_2 \in \mathbb{F}_{q^7}\}$$

or to

$$\mathcal{C}_7' := \{a_0X + a_1X^{q^3} + a_2X^{q^5} + a_3X^{q^6} : a_0, a_1, a_2, a_3 \in \mathbb{F}_{q^7}\}.$$

- *If $n = 8$ then $\mathcal{C}$ is equivalent to a generalized Gabidulin code or $q \equiv 1 \pmod 3$ and, up to the adjoint operation, $\mathcal{C}$ is equivalent either to*

$$\mathcal{C}_8 := \{a_0X + a_1X^q + a_2X^{q^3} : a_0, a_1, a_2 \in \mathbb{F}_{q^8}\}$$

or to

$$\mathcal{C}_8' := \{a_0X + a_1X^{q^2} + a_2X^{q^3} + a_3X^{q^4} + a_4X^{q^5} : a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_{q^8}\}.$$

(Note that $\mathcal{C}_7'$ is equivalent to $\mathcal{C}_7^\perp$ and $\mathcal{C}_8'$ is equivalent to $\mathcal{C}_8^\perp$.)

The rest of this paper is organized as follows: In Section 2, we prove several results concerning the representation and the equivalence of MRD codes with maximum left and right idealisers. Moreover, we also show connections between Moore matrices and such MRD codes. Section 3 includes the constructions and the classification results of Theorem 1.1. In Section 4 we show a link between the Dickson-Guralnick-Zieve curves and a family of rank-metric codes in $\mathbb{F}_q^{n\times n}$, which provides the MRD codes of Section 3 for $n = 7$ and 8. By using some recent results on these curves, we can prove that the members of this family of rank-metric codes are not MRD for $n \geq 9$.

2. Linearized polynomials and Moore matrices

As we are working with rank-distance codes in $\mathbb{F}_q^{n\times n}$ in this paper, it is more convenient to describe codes in the language of *q-polynomials* (or *linearized polynomials*) over $\mathbb{F}_{q^n}$, considered modulo $X^{q^n} - X$. These polynomials are represented by the set

$$\mathscr{L}_{(n,q)}[X] = \left\{ \sum_{i=0}^{n-1} c_i X^{q^i} : c_i \in \mathbb{F}_{q^n} \right\}.$$

After fixing an ordered $\mathbb{F}_q$-basis $\{b_1, b_2, \ldots, b_n\}$ for $\mathbb{F}_{q^n}$ it is possible to give a bijection Φ which associates for each matrix $M \in \mathbb{F}_q^{n\times n}$ a unique q-polynomial $f_M \in \mathscr{L}_{(n,q)}$. More precisely, put $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^n}^n$, then $\Phi(M) = f_M$ where for each $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ we have $f_M(\mathbf{b} \cdot \mathbf{u}) = \mathbf{b} \cdot \mathbf{u}M$. The trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined by the q-polynomial

$$\mathrm{Tr}_{q^n/q}(x) = x + x^q + \ldots + x^{q^{n-1}} \text{ for } x \in \mathbb{F}_{q^n}.$$

As we mentioned in the introduction, the most well-known family of MRD codes is called (generalized) Gabidulin codes. They can be described by the following subset of linearized polynomials:

$$\mathcal{G}_{k,s} = \{a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}, \tag{2}$$

where s is relatively prime to n. It is obvious that there are q^{kn} polynomials in $\mathcal{G}_{k,s}$. Each of them has at most q^{k-1} roots (cf. [22]) which means that this is an MRD code.

Given two rank-distance codes $\mathcal{C}_1$ and $\mathcal{C}_2$ which consist of linearized polynomials, they are equivalent if and only if there exist φ_1, $\varphi_2 \in \mathscr{L}_{(n,q)}[X]$ permuting $\mathbb{F}_{q^n}$, $\psi \in \mathscr{L}_{(n,q)}[X]$ and $\rho \in \mathrm{Aut}(\mathbb{F}_q)$ such that

$$\varphi_1 \circ f^\rho \circ \varphi_2 + \psi \in \mathcal{C}_2 \text{ for all } f \in \mathcal{C}_1,$$

where $\circ$ stands for the composition of maps and $f^\rho(X) = \sum a_i^\rho X^{q^i}$ for $f(X) = \sum a_i X^{q^i}$.

For a rank-distance code $\mathcal{C}$ given by a set of linearized polynomials, its left and right idealisers can be written as:

$$L(\mathcal{C}) = \{\varphi \in \mathscr{L}_{(n,q)} \colon f \circ \varphi \in \mathcal{C} \text{ for all } f \in \mathcal{C}\},$$

$$R(\mathcal{C}) = \{\varphi \in \mathscr{L}_{(n,q)} \colon \varphi \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}.$$

Note that the left idealiser is written as $f \circ \varphi$ rather than $\varphi \circ f$ because of the definition of Φ and similarly for the right idealiser.

The idealisers of generalized twisted Gabidulin codes together with a complete answer to the equivalence between members in this family can be found in [34].

The *adjoint* of a q-polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, with respect to the bilinear form $\langle x, y\rangle := \mathrm{Tr}_{q^n/q}(xy)$, is given by

$$\hat{f}(x) := \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}.$$

If $\mathcal{C}$ is a rank-metric code given by q-polynomials, then the *adjoint code* $\mathcal{C}^\top$ of $\mathcal{C}$ is $\{\hat{f} \colon f \in \mathcal{C}\}$.

In terms of linearized polynomials, the Delsarte dual can be interpreted in the following way [48]:

$$\mathcal{C}^\perp = \{f \colon b(f,g) = 0 \text{ for all } g \in \mathcal{C}\},$$

where $b(f,g) = \mathrm{Tr}_{q^n/q}\left(\sum_{i=0}^{n-1} a_i b_i\right)$ for $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$.

It is well-known and also not difficult to show directly that two linear rank-distance codes are equivalent if and only if their Delsarte duals or their adjoint codes are equivalent. This observation yields the following result which we will use without further mentioning throughout the paper.

Proposition 2.1. *Let $\mathcal{C}$ and $\mathcal{C}'$ be rank metric codes of $\mathbb{F}_q^{n\times n}$ such that $\mathcal{C}$ is obtained from $\mathcal{C}'$ via a finite combination (possibly with repetition) of the $\top$ and $\perp$ operations and the equivalence maps. Then $\mathcal{C}$ is equivalent to a generalized Gabidulin code if and only if $\mathcal{C}'$ is equivalent to a generalized Gabidulin code.*

Proof. It follows from the fact that $\mathcal{G}_{k,s}^\top$ is equivalent to $\mathcal{G}_{k,s}$ and $\mathcal{G}_{k,s}^\perp$ is equivalent to $\mathcal{G}_{n-k,s}$. □

Usually, codes equivalent to those defined in (2) are also called generalized Gabidulin codes. Note that changing the basis $\{b_1, b_2, \ldots, b_n\}$ of $\mathbb{F}_{q^n}$ can alter the shape of the corresponding q-polynomials but provide equivalent codes. In this paper by a generalized Gabidulin code we always refer to a code defined exactly as in (2). We decided along this notation since, as we will see, finding a nice shape of the representing q-polynomials has a crucial role in our investigation.

2.1. **Rank-distance codes with maximum nuclei.** First let us show that a rank-distance code in $\mathscr{L}_{(n,q)}$ with maximum right and left idealisers has to be equivalent to a set of linearized polynomials in a special form.

Theorem 2.2. *Let $\mathcal{C}$ be an $\mathbb{F}_q$-subspace of $\mathscr{L}_{(n,q)}$. Assume that one of the left and right idealisers of $\mathcal{C}$ is isomorphic to $\mathbb{F}_{q^n}$. Then there exists an integer k such that $|\mathcal{C}| = q^{kn}$ and $\mathcal{C}$ is equivalent to*

(3)
$$\mathcal{C} = \left\{ \sum_{i=0}^{k-1} a_i X^{q^{t_i}} + \sum_{j \notin \{t_0, t_1, \cdots, t_{k-1}\}}^{n-1} g_j(a_0, \cdots, a_{k-1}) X^{q^j} : a_0, \cdots, a_{k-1} \in \mathbb{F}_{q^n} \right\},$$

where $0 \le t_0 < t_1 < \cdots < t_{k-1} \le n-1$ and the g_j's are $\mathbb{F}_q$-linear functions from $\mathbb{F}_{q^n}^k$ to $\mathbb{F}_{q^n}$. If the other idealiser of $\mathcal{C}$ is also isomorphic to $\mathbb{F}_{q^n}$, then $\mathcal{C}$ is equivalent to

$$\left\{ \sum_{i=0}^{k-1} a_i X^{q^{t_i}} : a_i \in \mathbb{F}_{q^n} \right\}. \tag{4}$$

Proof. Let $\mathcal{N}$ denote the idealiser of $\mathcal{C}$ which is isomorphic to $\mathbb{F}_{q^n}$. All Singer cycles in $\mathrm{GL}(n,q)$ are conjugate, i.e. there exists an invertible $f \in \mathscr{L}_{(n,q)}$ such that $\mathcal{N}' := f \circ \mathcal{N} \circ f^{-1} = \{aX : a \in \mathbb{F}_{q^n}\}$. It follows that when $\mathcal{N} = R(\mathcal{C})$ then $R(\mathcal{C}') = \mathcal{N}'$ where $\mathcal{C}' = f \circ \mathcal{C}$, whereas when $\mathcal{N} = L(\mathcal{C})$ then $L(\mathcal{C}') = \mathcal{N}'$ where $\mathcal{C}' = \mathcal{C} \circ f^{-1}$. It means that up to equivalence we may assume that

$$\mathcal{N} = \{aX : a \in \mathbb{F}_{q^n}\}. \tag{5}$$

If the other idealiser $\mathcal{M}$ of $\mathcal{C}$ is also isomorphic to $\mathbb{F}_{q^n}$, then by using another equivalence map we may also assume that $\mathcal{M} = \mathcal{N}$.

First we prove (3). Let t_0 be an integer such that there exists $f_0(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathcal{C}$ with $a_{t_0} \neq 0$. If $\mathcal{N}$ is the right idealiser of $\mathcal{C}$, then, by (5), $\{af_0(X) : a \in \mathbb{F}_{q^n}\} \subseteq \mathcal{C}$, which means that for any $a \in \mathbb{F}_{q^n}$ there is at least one polynomial in $\mathcal{C}$ where the coefficient of $X^{q^{t_0}}$ equals a. If $\mathcal{N}$ is the left idealiser of $\mathcal{C}$, then, by (5), $\{f_0(aX) : a \in \mathbb{F}_{q^n}\} \subseteq \mathcal{C}$. Again, it follows that for any $a \in \mathbb{F}_{q^n}$ there is at least one polynomial in $\mathcal{C}$ in which the coefficient of $X^{q^{t_0}}$ equals a.

If $|\mathcal{C}| = q^n$, we have proved (3); otherwise there exist non-zero polynomials in $\mathcal{C}$ where the coefficient of $X^{q^{t_0}}$ is 0. Let us denote the set of all such polynomials by $\bar{\mathcal{C}}$. It is easy to check that $\bar{\mathcal{C}}$ is still an $\mathbb{F}_q$-subspace. Let $t_1 \neq t_0$ be an integer such that there exists a polynomial $f_1(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \bar{\mathcal{C}}$ with $a_{t_1} \neq 0$. Again, if $\mathcal{N} = R(\mathcal{C})$, by (5), we see that $\{af_1(X) : a \in \mathbb{F}_{q^n}\} \subseteq \bar{\mathcal{C}}$, whence $\{a_0 f_0(X) + a_1 f_1(X) : a_0, a_1 \in \mathbb{F}_{q^n}\} \subseteq \mathcal{C}$. If $\mathcal{N} = L(\mathcal{C})$ then $\{f_1(aX) : a \in \mathbb{F}_{q^n}\} \subseteq \bar{\mathcal{C}}$ which means $\{f_0(a_0 X) + f_1(a_1 X) : a_0, a_1 \in \mathbb{F}_{q^n}\} \subseteq \mathcal{C}$. If $|\mathcal{C}| = q^{2n}$, we have proved (3); otherwise we continue this process by choosing a suitable $t_2 \notin \{t_0, t_1\}$ and so on. After finite steps, we obtain $|\mathcal{C}| = q^{kn}$ and (3).

Now we prove (4), so suppose that the other idealiser $\mathcal{M}$ is also isomorphic to $\mathbb{F}_{q^n}$. As we already mentioned, we may assume

$$\mathcal{M} = \{aX : a \in \mathbb{F}_{q^n}\}. \tag{6}$$

By (3),

$$f(X) = c_0 X^{q^{t_0}} + \sum_{j \notin \{t_0, \ldots, t_{k-1}\}}^{n-1} g_j(c_0, 0, \ldots, 0) X^{q^j} \in \mathcal{C},$$

for each $c_0 \in \mathbb{F}_{q^n}$. For any $b \in \mathbb{F}_{q^n}^*$, it is clear that $\varphi_2(X) := bX \in L(\mathcal{C})$ and $\varphi_1(X) := b^{-q^{t_0}}X \in R(\mathcal{C})$. Then

$$\varphi_1 \circ f \circ \varphi_2(X) = c_0 X^{q^{t_0}} + \sum_{j \notin \{t_0,\ldots,t_{k-1}\}}^{n-1} g_j(c_0, 0, \ldots, 0) b^{q^j - q^{t_0}} X^{q^j} \in \mathcal{C}.$$

Since f is the unique element in $\mathcal{C}$ associated with $(a_0, \ldots, a_{k-1}) = (c_0, 0, \ldots, 0)$ we have

$$g_j(c_0, 0, \ldots, 0) b^{q^j - q^{t_0}} = g_j(c_0, 0, \ldots, 0)$$

for every $b \in \mathbb{F}_{q^n}$, which implies that $g_j(c_0, 0, \ldots, 0) = 0$ for every $j \notin \{t_0, \ldots, t_{k-1}\}$ and for each $c_0 \in \mathbb{F}_{q^n}$. Similarly, we can prove that $g_j(0, \ldots, c_i, \ldots, 0) = 0$ for every $i \in \{0, \ldots, k-1\}$, $j \notin \{t_0, \ldots, t_{k-1}\}$ and $c_i \in \mathbb{F}_{q^n}$. Since $g_j(a_0, \ldots, a_{k-1}) = g_j(a_0, 0, \ldots) + g_j(0, a_1, 0, \ldots) + \cdots + g_j(0, \ldots, a_{k-1})$, g_j is the zero map for each j. Therefore we obtain (4). □

The next result shows how to handle the equivalence problem of MRD codes given as in (4).

Theorem 2.3. *Let Λ_1 and Λ_2 be two k-subsets of $\{0, \ldots, n-1\}$. Define*

$$\mathcal{C}_j = \left\{ \sum_{i \in \Lambda_j} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n} \right\}$$

for $j = 1, 2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if and only if

$$\Lambda_2 = \Lambda_1 + s := \{i + s \pmod n : i \in \Lambda_1\} \tag{7}$$

for some $s \in \{0, \cdots, n-1\}$.

Proof. The if part is trivial since $\Lambda_2 = \Lambda_1 + s$ implies $\mathcal{C}_2 = X^{q^s} \circ \mathcal{C}_1$. Assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. Let $\tau = (\varphi_1, \varphi_2, \rho)$ denote an equivalence map from $\mathcal{C}_1$ to $\mathcal{C}_2$, i.e.

$$\{\varphi_1 \circ f^\rho \circ \varphi_2 : f \in \mathcal{C}_1\} = \mathcal{C}_2.$$

For every $j \in \{0, \cdots, n-1\}$, let $\mathcal{D}_j = \{aX^{q^j} : a \in \mathbb{F}_{q^n}\}$. Define

$$I_j = \{i : \text{the coefficient of } X^{q^i} \text{ in } \varphi_1 \circ g^\rho \circ \varphi_2(X) \text{ is non-zero for some } g \in \mathcal{D}_j\}.$$

Since $\varphi_1 \circ g^\rho \circ \varphi_2$ is the zero polynomial only when g is the zero polynomial, it follows that $I_j \neq \emptyset$ for each j. By [34, Lemma 4.5], for any $j, l \in \{0, \cdots, n-1\}$,

$$I_l = I_j + l - j := \{i + l - j \pmod n : i \in I_j\}.$$

If $l \in \Lambda_1$, then $\mathcal{D}_l \subseteq \mathcal{C}_1$ and hence $I_l \subseteq \Lambda_2$. Take any $s \in I_0$ and $l \in \Lambda_1$, then $s + l \in I_0 + l = I_l \subseteq \Lambda_2$ and hence by $|\Lambda_1| = |\Lambda_2| = k$ we obtain $\Lambda_2 = \Lambda_1 + s$. □

2.2. **Links with Moore Matrices.** It is clear that generalized Gabidulin codes and codes equivalent to them have maximum idealisers. It is not difficult to verify that they are actually the only known examples with this property. Hence, it is natural to ask whether there are MRD codes, inequivalent to the generalized Gabidulin codes, which have maximum idealisers. If they exist, can we classify them?

This question also has an interesting link with Moore matrices and Moore determinants which were introduced by Moore [39] in 1896.

Let q be a prime power and take two positive integers, n and s, with $\gcd(n,s)=1$. Put $\sigma := q^s$. For $A := \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$, $k \leq n$, a *square Moore matrix* is defined as

$$M_{A,\sigma} := \begin{pmatrix} \alpha_0 & \alpha_0^{\sigma} & \cdots & \alpha_0^{\sigma^{k-1}} \\ \alpha_1 & \alpha_1^{\sigma} & \cdots & \alpha_1^{\sigma^{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k-1} & \alpha_{k-1}^{\sigma} & \cdots & \alpha_{k-1}^{\sigma^{k-1}} \end{pmatrix}, \tag{8}$$

which is a σ-analogue for the Vandermonde matrix. When it is clear from the context, then σ will be omitted and we will simply write M_A. When $s=1$, then the determinant of M can be expressed as

$$\det(M_A) = \prod_{\mathbf{c}} (c_0\alpha_0 + c_1\alpha_1 + \cdots c_{k-1}\alpha_{k-1}), \tag{9}$$

where $\mathbf{c} = (c_0, c_1, \cdots, c_{k-1})$ runs over all direction vectors in $\mathbb{F}_q^k$, or equivalently we can say that $\mathbf{c}$ runs over $\mathrm{PG}(k-1,q)$. We call $\det(M_A)$ the *Moore determinant*. It is not difficult to see that the following generalization also holds. (In Remark 1 we will show how this result follows also from our Theorem 2.5.)

Theorem 2.4. *Assume that s satisfies $\gcd(s,n)=1$. For any $A = \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$, $k \leq n$, the elements of A are $\mathbb{F}_q$-linearly dependent if and only if $\det(M_A) = 0$.*

Assume $\gcd(s,n)=1$ and take any set of pairwise distinct integers $\mathcal{T} = \{t_0, t_1, \ldots, t_{k-1}\}$ with $0 \leq t_0 < t_1 < \ldots < t_{k-1} < n$ and $A = \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$, $k \leq n$. Put $\sigma = q^s$ and let

$$M_{\mathcal{T},A,\sigma} := \begin{pmatrix} \alpha_0^{\sigma^{t_0}} & \alpha_0^{\sigma^{t_1}} & \cdots & \alpha_0^{\sigma^{t_{k-1}}} \\ \alpha_1^{\sigma^{t_0}} & \alpha_1^{\sigma^{t_1}} & \cdots & \alpha_1^{\sigma^{t_{k-1}}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k-1}^{\sigma^{t_0}} & \alpha_{k-1}^{\sigma^{t_1}} & \cdots & \alpha_{k-1}^{\sigma^{t_{k-1}}} \end{pmatrix}. \tag{10}$$

As before, σ will be omitted when it is clear from the context. It is easy to see that if the elements of A are $\mathbb{F}_q$-linearly dependent, then $\det(M_{\mathcal{T},A}) = 0$. Regarding the other direction we have the following.

Theorem 2.5. *Assume that s satisfies $\gcd(s,n)=1$ and put $\sigma = q^s$. The set of q-polynomials*

$$\{a_0X^{\sigma^{t_0}} + a_1X^{\sigma^{t_1}} + \ldots + a_{k-1}X^{\sigma^{t_{k-1}}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\} \tag{11}$$

is an MRD code (with maximum idealisers) if and only if for any $A = \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$, $k \leq n$, $\det(M_{\mathcal{T},A}) = 0$ implies that the elements of A are $\mathbb{F}_q$-linearly dependent.

Proof. Note that $\det(M_{\mathcal{T},A}) = 0$ for some k-subset $A \subseteq \mathbb{F}_{q^n}$ if and only if the columns of $M_{\mathcal{T},A}$ are dependent over $\mathbb{F}_{q^n}$ which holds if and only if there exist $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}$, not all of them zero, such that

$$\sum_{j=0}^{k-1} \alpha_i^{\sigma^{t_j}} a_j = 0$$

holds for $i \in \{0, 1, \ldots, k-1\}$. Equivalently, the elements of A are roots of

$$a_0 X^{\sigma^{t_0}} + a_1 X^{\sigma^{t_1}} + \ldots + a_{k-1} X^{\sigma^{t_{k-1}}}. \tag{12}$$

If (11) is an MRD code, then (12) cannot have q^k roots and hence for any k-subset A of $\mathbb{F}_q$-linearly independent elements we obtain $\det(M_{\mathcal{T},A}) \neq 0$.

On the other hand, if $\mathcal{T}$ has been choosen such that $\det(M_{\mathcal{T},A}) = 0$ implies the $\mathbb{F}_q$-dependence of the elements in A for any k-subset $A \subseteq \mathbb{F}_{q^n}$, then the non-zero polynomials of (11) have less than q^k roots and hence (11) is an MRD code.

By Theorem 2.2, if (11) is an MRD code, then it has maximum idealisers. □

Remark 1. It follows from Theorem 2.5 with $t_i = i$ for $i \in \{0, 1, \ldots, k-1\}$ that Moore's Theorem 2.4 is equivalent to the fact that generalized Gabidulin codes are MRD codes.

For a k-subset $\mathcal{T}$ of $\{0, 1, \ldots, n-1\}$, let $V_{\mathcal{T}}$ denote the hypersurface of $\mathrm{PG}(k-1, \mathbb{K})$, where $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_q$, defined by the polynomial

$$\det \begin{pmatrix} X_0^{\sigma^{t_0}} & X_0^{\sigma^{t_1}} & \cdots & X_0^{\sigma^{t_{k-1}}} \\ X_1^{\sigma^{t_0}} & X_1^{\sigma^{t_1}} & \cdots & X_1^{\sigma^{t_{k-1}}} \\ \vdots & \vdots & \ddots & \vdots \\ X_{k-1}^{\sigma^{t_0}} & X_{k-1}^{\sigma^{t_1}} & \cdots & X_{k-1}^{\sigma^{t_{k-1}}} \end{pmatrix} \in \mathbb{F}_q[X_0, X_1, \ldots, X_{k-1}].$$

The following will be used in Section 4 to prove the nonexistence result.

Theorem 2.6. *Fix $\sigma = q^s$ where s is an integer such that $\gcd(s, n) = 1$. Let $\mathcal{S} = \{s_0, s_1, \ldots, s_{k-1}\}$ and $\mathcal{T} = \{t_0, t_1, \ldots, t_{k-1}\}$ be two subsets of $\{0, 1, \ldots, n-1\}$ and suppose that*

$$\mathcal{C}_{\mathcal{T}} := \{a_0 X^{\sigma^{t_0}} + a_1 X^{\sigma^{t_1}} + \ldots + a_{k-1} X^{\sigma^{t_{k-1}}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is an MRD code. Then

$$\mathcal{C}_{\mathcal{S}} := \{a_0 X^{\sigma^{s_0}} + a_1 X^{\sigma^{s_1}} + \ldots + a_{k-1} X^{\sigma^{s_{k-1}}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is an MRD code if and only if there are no $\mathbb{F}_{q^n}$-rational points in $V_{\mathcal{S}} \setminus V_{\mathcal{T}}$.

Proof. According to Theorem 2.5 the $\mathbb{F}_{q^n}$-rational points of $V_{\mathcal{T}}$ are

$$\mathcal{L} := \{\langle(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})\rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(k-1, q^n) \colon \dim\langle\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\rangle_{\mathbb{F}_q} < k\}.$$

If $\mathcal{C}_{\mathcal{S}}$ is also an MRD code, then again from Theorem 2.5 the set of $\mathbb{F}_{q^n}$-rational points of $V_{\mathcal{S}}$ coincides with the point set $\mathcal{L}$. On the other hand if there exists $\langle(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})\rangle_{\mathbb{F}_{q^n}} \in V_{\mathcal{S}} \setminus V_{\mathcal{T}}$, then $\dim\langle\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\rangle_{\mathbb{F}_q} = k$ and with $A = \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ we have $\det(M_{\mathcal{S},A}) = 0$. Theorem 2.5 yields that $\mathcal{C}_{\mathcal{S}}$ is not an MRD code. □

3. Constructions and classifications

In this section our aim is to classify $\mathbb{F}_q$-linear MRD codes with maximum idealisers in $\mathbb{F}_q^{n \times n}$ with $n \leq 9$. In terms of linearized polynomials, by Theorem 2.2 it is equivalent to find k-subsets $\mathcal{T} := \{t_0, t_1, \ldots, t_{k-1}\}$ of $\{0, 1, \ldots, n-1\}$ such that the non-zero polynomials in

$$\mathcal{C}_{\mathcal{T}} := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

have at most q^k roots.

Clearly, if $k = 1$, then we obtain generalized Gabidulin codes with minimum distance n.

Proposition 3.1. *Let $\mathcal{T} = \{t_0, t_1, \ldots, t_{k-1}\} \subseteq \{0, 1, \ldots, n-1\}$. If $\mathcal{C}_\mathcal{T}$ is an MRD code then $\gcd(t_i - t_j, n) < k$ for each $i \neq j$, $i, j \in \{0, 1, \ldots, k-1\}$.*

Proof. We may assume $t_j < t_i$ and put $s = \gcd(t_j - t_i, n)$. It is enough to observe that the elements of $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^n}$ are roots of $(X^{q^{t_i - t_j}} - X)^{q^{t_j}} \in \mathcal{C}_\mathcal{T}$ and hence if $s \geq k$, then $\mathcal{C}_\mathcal{T}$ is not an MRD code. □

If $k = 2$, then by Proposition 3.1 we have to consider polynomials of the form

$$\{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} : a_0, a_1 \in \mathbb{F}_{q^n}\},$$

with $\gcd(t_1 - t_0, n) = 1$. These codes are clearly equivalent to generalized Gabidulin codes.

Applying Delsarte dual operation we may always assume $k \leq n/2$, since $\mathcal{C}_\mathcal{T}^\perp = \mathcal{C}_{\mathcal{T}'}$ where $\mathcal{T}' = \{0, 1, \ldots, n-1\} \setminus \mathcal{T}$. As $\mathcal{C}_\mathcal{T}$ is equivalent to $\mathcal{C}_{\mathcal{T}'}$ (cf. Theorem 2.3) for every $\mathcal{T}' = \mathcal{T} + s := \{t + s \pmod n : t \in \mathcal{T}\}$, we may also assume $0 \in \mathcal{T}$.

Applying now the adjoint operation we may further assume that for $k > 1$ there exists $1 \leq i \leq n/2$ such that $i \in \mathcal{T}$. This is because if $0 \in \mathcal{T}$ then $\mathcal{C}_\mathcal{T}^\top = \mathcal{C}_{\mathcal{T}'}$ where $\mathcal{T}' = \{0\} \cup \{n - i : i \in \mathcal{T},\ i \neq 0\}$.

It follows that for $n \leq 5$ the MRD codes with both idealisers isomorphic to $\mathbb{F}_{q^n}$ are equivalent to generalized Gabidulin codes.

Now consider $n = 6$ and $k = 3$. It is enough to consider polynomial subspaces of the form

$$\{a_0 X + a_1 X^{q^{t_1}} + a_2 X^{q^{t_2}} : a_0, a_1, a_2 \in \mathbb{F}_{q^6}\},$$

with $t_1 \in \{1, 2\}$ and $t_1 < t_2$. From Proposition 3.1 we have $\gcd(t_2, 6) \leq 2$ and $\gcd(t_2 - t_1, 6) \leq 2$. If $t_1 = 1$ then we get $t_2 \in \{2, 5\}$ and both cases yield codes equivalent to Gabidulin codes. If $t_1 = 2$ then $t_2 = 4$ but then $\mathrm{Tr}_{q^6/q^2}(X)$ is in the code, a contradiction since it has q^4 roots in $\mathbb{F}_{q^6}$. Thus we have proved the following.

Proposition 3.2. *If $n \leq 6$ then MRD codes with both idealisers isomorphic to $\mathbb{F}_{q^n}$ are equivalent to generalized Gabidulin codes.*

Using a similar argument together with Theorem 2.3, we can exclude most of the possibilities also for $n = 7, 8, 9$ and obtain that, up to $\perp$ and $\top$ operations if an MRD code $\mathcal{C}_\mathcal{T}$ with $\mathcal{T} \subseteq \{0, 1, \ldots, n-1\}$ has maximum left and right idealisers and it is not equivalent to generalized Gabidulin codes then up to equivalence it has to have one of the following form:

(1) $n \in \{7, 8\}$, $k = 3$ and $\mathcal{T} = \{0, 1, 3\}$,
(2) $n = 9$, $k = 4$ and $\mathcal{T} = \{0, s, 2s, 4s\}$, where $s \in \{1, 4, 7\}$ and the elements of $\mathcal{T}$ are considered modulo 9.

As we will see, in the first case we have MRD codes under certain conditions on q while in the second case we never obtain MRD codes.

We recall the following result on q-polynomials which we will use frequently. Let $f(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ with $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_{q^n}$ and let D_f denote the associated

Dickson matrix (or *q-circulant matrix*)

$$D_f := \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix}.$$

Then the rank of D_f equals the rank of f viewed as an $\mathbb{F}_q$-linear transformation of $\mathbb{F}_{q^n}$, see for example [53].

3.1. The $n = 7$ case.

Theorem 3.3. *The set of q-polynomials*

$$\mathcal{C}_7 := \{a_0X + a_1X^q + a_2X^{q^3} : a_0, a_1, a_2 \in \mathbb{F}_{q^7}\} \tag{13}$$

is an $\mathbb{F}_q$-linear MRD code with left and right idealisers isomorphic to $\mathbb{F}_{q^7}$ if and only if q is odd. Moreover, $\mathcal{C}_7$ is not equivalent to the previously known MRD codes.

Proof. The Dickson matrix associated with $f(X) = X + X^q + X^{q^3} \in \mathbb{F}_{q^7}[X]$ is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This matrix can also be viewed as the incidence matrix of the points and lines of $\mathrm{PG}(2, 2)$. It is well-known, and also easy to see, that it has rank four over $\mathbb{F}_2$, hence $f(X)$ has q^3 roots, i.e. $\mathcal{C}_7$ is not an MRD code.

Now let q be odd and suppose to the contrary that $\mathcal{C}_7$ is not an MRD code. Then there exist $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{q^7}$ such that $\alpha_1X + \alpha_2X^q + \alpha_3X^{q^3}$ has q^3 roots. Clearly these roots form an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^7}$, let u_1, u_2, u_3 be an $\mathbb{F}_q$-basis for this subspace.

Let σ denote the collineation of $\mathrm{PG}(2, q^7)$ defined by the following semilinear map of $\mathbb{F}_{q^7}^3$: $(x_1, x_2, x_3) \mapsto (x_1^q, x_2^q, x_3^q)$. Let $\Sigma \cong \mathrm{PG}(2, q)$ denote the points of $\mathrm{PG}(2, q^7)$ fixed by σ. Define $P := \langle (u_1, u_2, u_3) \rangle_{\mathbb{F}_{q^7}}$ and note that $P \notin \Sigma$, otherwise $\lambda(u_1, u_2, u_3) = (u_1^q, u_2^q, u_3^q)$ for some $\lambda \in \mathbb{F}_{q^7}^*$, a contradiction since this would mean that $u_1^{q-1} = u_2^{q-1} = u_3^{q-1}$, i.e. $\dim\langle u_1, u_2, u_3\rangle_{\mathbb{F}_q} = 1$. It follows that P lies on an orbit of length seven of σ.

The scalars $\alpha_1, \alpha_2, \alpha_3$ show that the columns of the matrix

$$M := \begin{pmatrix} u_1 & u_1^q & u_1^{q^3} \\ u_2 & u_2^q & u_2^{q^3} \\ u_3 & u_3^q & u_3^{q^3} \end{pmatrix}$$

are $\mathbb{F}_{q^7}$-linearly dependent and hence also the rows of M are $\mathbb{F}_{q^7}$-linearly dependent, which shows that there exists a line ℓ of $\mathrm{PG}(2, q^7)$ which is incident with P, P^σ and P^{σ^3}.

First we show that ℓ is not a line of Σ, which is equivalent to say $\ell \neq \ell^\sigma$. Suppose the contrary, then ℓ has an equation $a_1X_1 + a_2X_2 + a_3X_3 = 0$ where X_1, X_2, X_3

denote the homogeneous coordinates for points of $\mathrm{PG}(2,q^7)$ and $a_1,a_2,a_3\in\mathbb{F}_q$. A contradiction since $\dim\langle u_1,u_2,u_3\rangle_{\mathbb{F}_q}=3$.

Next we show that ℓ cannot be tangent to Σ. Suppose to the contrary that $\ell\cap\Sigma=\{Q\}$ for some point Q. Then $Q\in\ell\cap\ell^\sigma=\{P^\sigma\}$, a contradiction since $\{P,P^\sigma,P^{\sigma^2},\dots,P^{\sigma^6}\}$ are not fixed by σ hence $P^\sigma=Q$ cannot be a point of Σ.

Thus ℓ lies on an orbit of length 7 of σ and since $\{0,1,3\}$ is a cyclic $(7,3,1)$-difference set of $\mathbb{Z}_7$, the cyclic group of order 7 (written additively), we have that the points $\{P,P^\sigma,P^{\sigma^2},\dots,P^{\sigma^6}\}$ and lines $\{\ell,\ell^\sigma,\dots,\ell^{\sigma^6}\}$ form a Fano subplane inside $\mathrm{PG}(2,q^7)$. However, it is well known that a Fano plane cannot be embedded in $\mathrm{PG}(2,q)$ if q is odd. Thus we get a contradiction.

The last part follows from Theorem 2.3 and from the fact that the only known MRD codes with maximum left and right idealisers are equivalent to the generalized Gabidulin codes. □

As observed in Section 2, the Delsarte dual operation preserves the equivalence relations between MRD codes. Hence we have the following result.

Corollary 3.4. *The set of q-polynomials*

$$\mathcal{C}'_7:=\{a_0X+a_1X^{q^3}+a_2X^{q^5}+a_3X^{q^6}:a_0,a_1,a_2,a_3\in\mathbb{F}_{q^7}\} \tag{14}$$

is an $\mathbb{F}_q$-linear MRD code with left and right idealisers isomorphic to $\mathbb{F}_{q^7}$ if and only if q is odd. Moreover, $\mathcal{C}'_7$ is not equivalent to the previously known MRD codes.

3.2. The $n=8$ case.

Theorem 3.5. *The set of q-polynomials*

$$\mathcal{C}_8:=\{a_0X+a_1X^q+a_2X^{q^3}:a_0,a_1,a_2\in\mathbb{F}_{q^8}\} \tag{15}$$

is an $\mathbb{F}_q$-linear MRD code with left and right idealisers isomorphic to $\mathbb{F}_{q^8}$ if and only if $q\equiv 1 \pmod 3$. Moreover, $\mathcal{C}_8$ is not equivalent to the previously known MRD codes.

Proof. First suppose $q\not\equiv 1 \pmod 3$ and choose a such that $1+a+a^2=0$. If $q\equiv -1 \pmod 3$, then $a\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $a^q=1/a$. If $q\equiv 0 \pmod 3$, then $a=1$. Note that the Dickson matrix associated with $X+X^q+aX^{q^3}\in\mathbb{F}_{q^8}[X]$ is

$$M:=\begin{pmatrix}
1 & 1 & 0 & a & 0 & 0 & 0 & 0\\
0 & 1 & 1 & 0 & 1/a & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 0 & a & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 1/a & 0\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & a\\
1/a & 0 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & a & 0 & 0 & 0 & 0 & 1 & 1\\
1 & 0 & 1/a & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

whose last five columns are linearly independent and hence the rank of M is at least 5.

If the characteristic of $\mathbb{F}_q$ is 3, then the rows of M are orthogonal to the rows of

$$\begin{pmatrix}
2 & 0 & 1 & 1 & 2 & 1 & 0 & 0\\
2 & 2 & 1 & 2 & 0 & 0 & 1 & 0\\
0 & 2 & 2 & 1 & 2 & 0 & 0 & 1
\end{pmatrix},$$

which is a matrix of rank 3. It follows that in this case the rank of M is 5.

On the other hand, if $q \equiv -1 \pmod 3$, then the matrix

$$\begin{pmatrix} 1 & a & a^2 & a & a & a^2 & -2a^2 & a^2 \\ a & 1 & a^2 & a & a^2 & a^2 & a & -2a \\ -2a^2 & a^2 & 1 & a & a^2 & a & a & a^2 \end{pmatrix}$$

has rank three and its rows are orthogonal to the rows of M, thus M has rank 5.

Now let $q \equiv 1 \pmod 3$ and suppose to the contrary that $\mathcal{C}_8$ is not an MRD code. Then arguing as in the proof of Theorem 3.3, there exist $\mathbb{F}_q$-linearly independent elements $u_1, u_2, u_3 \in \mathbb{F}_{q^8}$ and a line ℓ of $\mathrm{PG}(2, q^8)$ incident with $P := \langle (u_1, u_2, u_3) \rangle$ and with P^σ, P^{σ^3}, where σ is the collineation of $\mathrm{PG}(2, q^8)$ defined by the semilinear map $(x_1, x_2, x_3) \mapsto (x_1^q, x_2^q, x_3^q)$. Also, let $\Sigma \cong \mathrm{PG}(2, q)$ denote the set of points of $\mathrm{PG}(2, q^8)$ fixed by σ. Since $P, P^\sigma, P^{\sigma^3}$ are three different points and since $\ell \cap \Sigma = \emptyset$, P^{σ^2} and P^{σ^5} are two further points, which are not incident with ℓ. So, if $T := \langle P^\sigma, P^{\sigma^2} \rangle \cap \langle P, P^{\sigma^5} \rangle$, then P, P^{σ^2}, P^{σ^3} and T are four points no three of which are collinear. Hence, there exists a projectivity φ of $\mathrm{PG}(2, q^8)$ such that

$$P^\varphi = \langle (0,0,1) \rangle =: P_0, \quad P^{\sigma^3\varphi} = \langle (0,1,0) \rangle =: P_3, \quad P^{\sigma^2\varphi} = \langle (1,0,0) \rangle =: P_2$$

and $\langle (1,1,1) \rangle$ is the point T^φ. In this way

$$P^{\sigma\varphi} = \langle (0,1,1) \rangle =: P_1, \quad P^{\sigma^5\varphi} = \langle (1,1,0) \rangle =: P_5, \quad P^{\sigma^6\varphi} = \langle (a,a,1) \rangle =: P_6$$

for some $a \in \mathbb{F}_{q^8}^*$. Also, elementary calculations show

$$P^{\sigma^7\varphi} = \langle (a, 0, 1-a) \rangle =: P_7, \quad \text{and} \quad P^{\sigma^4\varphi} = \langle (1, 1-a, 1-a) \rangle =: P_4.$$

Since P_3, P_4, P_6 are collinear, it follows that

$$a^2 - a + 1 = 0, \tag{16}$$

and hence, since $q \equiv 1 \pmod 3$, we get $a \in \mathbb{F}_q$. Let $\bar{\sigma} = \varphi \circ \sigma \circ \varphi^{-1}$. Then $\bar{\sigma}$ is a collineation of order 8 of $\mathrm{PG}(2, q^8)$ and it is induced by a semilinear map of this form

$$(x_1, x_2, x_3) \mapsto \left(\sum_{j=1}^3 a_{1j} x_j^q, \sum_{j=1}^3 a_{2j} x_j^q, \sum_{j=1}^3 a_{3j} x_j^q \right),$$

with (a_{ij}) a non-singular 3×3 matrix over $\mathbb{F}_{q^8}$. By construction, it is easy to see that $P_i^{\bar{\sigma}} = P_{i+1}$, for $i = 0, \ldots, 7 \pmod 8$. Direct computations for $i = 0, 1, 2, 4$ show that up to a scalar of $\mathbb{F}_{q^8}^*$

$$(a_{ij}) = \begin{pmatrix} 0 & 1 & 0 \\ 1-a & 1-a & a-1 \\ 0 & 1-a & a-1 \end{pmatrix}$$

and from $P_5^{\bar{\sigma}} = P_6$ we get $1 = 2 - 2a$. This clearly cannot hold if q is even, while for q odd it gives $a = 1/2$ which does not satisfy (16), a contradiction.

The last part follows as in Theorem 3.3. □

Again, since the Delsarte dual operation preserves the equivalence relations between MRD codes, we have the following result.

Corollary 3.6. *The set of q-polynomials*

$$\mathcal{C}'_8 := \{a_0X + a_1X^{q^2} + a_2X^{q^3} + a_3X^{q^4} + a_4X^{q^5} : a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_{q^8}\} \tag{17}$$

is an $\mathbb{F}_q$-linear MRD code with left and right idealisers isomorphic to $\mathbb{F}_{q^8}$ if and only if $q \equiv 1 \pmod 3$. Moreover, $\mathcal{C}'_8$ is not equivalent to the previously known MRD codes.

3.3. **The $n = 9$ case.** For $s \in \{1, 4, 7\}$ consider the rank codes

$$\mathcal{D}_s := \{a_0X + a_1X^{q^s} + a_2X^{q^{2s}} + a_3X^{q^{4s}} : a_0, a_1, a_2, a_3 \in \mathbb{F}^*_{q^9}\}.$$

First we show that $\mathcal{D}_1$ is not an MRD code.

Put $f(X) := -X + (1 + c^{-q})X^q + cX^{q^2} - X^{q^4} \in \mathcal{D}_1$ with $c \in \mathbb{F}^*_{q^3}$ such that $\mathrm{Tr}_{q^3/q}(1/c) = -2$ and $\mathrm{N}_{q^3/q}(1/c) = -1$. Here $\mathrm{N}_{q^n/q}(x) = x^{1+q+\ldots+q^{n-1}}$ denotes the norm of $x \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. By [37, Theorem 5.3] we can find such an element c in $\mathbb{F}^*_{q^3}$. Let $D_f = (d_{ij})$ denote the Dickson matrix associated with f. Substituting $-c^{-q-1}$ for c^{q^2} at positions d_{35}, d_{68} and d_{92} we obtain

$$D_f = \begin{pmatrix}
-1 & \alpha & c & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & -1 & \beta & c^q & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & -1 & \gamma & -c^{-q-1} & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & -1 & \alpha & c & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & -1 & \beta & c^q & 0 & -1 \\
-1 & 0 & 0 & 0 & 0 & -1 & \gamma & -c^{-q-1} & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & -1 & \alpha & c \\
c^q & 0 & -1 & 0 & 0 & 0 & 0 & -1 & \beta \\
\gamma & -c^{-q-1} & 0 & -1 & 0 & 0 & 0 & 0 & -1
\end{pmatrix},$$

with $\alpha = 1 + c^{-q}$, $\beta = -1 - c^{-1} - c^{-q}$ and $\gamma = 1 + 1/c$, where β is obtained after substituting $-1-c^{-1}-c^{-q}$ for $1+c^{-q^2}$. The 5×5 submatrix M formed by the first five rows and the first five columns of D_f is triangular with non-zero entries on its diagonal, hence it is non-singular. Then the rank of D_f is five if and only if all the 6×6 submatrices of D_f which contain M are singular (this is an exercise in linear algebra and we omit its proof). We have 16 such submatrices and we consider their determinants as polynomials in c. By calculation, it turns out that each of them is divisible by

$$c^{2q+2} - 2c^{q+1} - c^q - c. \tag{18}$$

Note that $\mathrm{N}_{q^3/q}(c) = -1$ and hence $\mathrm{Tr}_{q^3/q}(c^{q+1}) = \mathrm{Tr}_{q^3/q}(1/c)\mathrm{N}_{q^3/q}(c) = 2$. Multiplying (18) by c^{q^2} gives $-\mathrm{Tr}_{q^3/q}(c^{q+1}) + 2 = 0$ thus D_f has rank five. It follows that $f(X)$ has q^4 roots and hence $\mathcal{D}_1$ is not an MRD code.

Now let

$$K := \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Since f has coefficients in $\mathbb{F}_{q^3}$, it is easy to see that KD_fK^{-1} is the Dickson matrix associated with $-X+(1+c^{-q})X^{q^4}+cX^{q^8}-X^{q^7} \in \mathcal{D}_4$ and $K^2D_fK^{-2}$ is the Dickson matrix associated with $-X+(1+c^{-q})X^{q^7}+cX^{q^5}-X^q \in \mathcal{D}_7$. It follows that these two polynomials have q^4 roots as well and hence $\mathcal{D}_4$ and $\mathcal{D}_7$ are not MRD codes, and we have proven the following result.

Proposition 3.7. *If $n = 9$ then MRD codes with both idealisers isomorphic to $\mathbb{F}_{q^9}$ are equivalent to generalized Gabidulin codes.*

Proof of Theorem 1.1. The result follows from Proposition 3.2, the discussions after Proposition 3.2, Theorem 3.3, Corollary 3.4, Theorem 3.5, Corollary 3.6 and Proposition 3.7. □

4. Nonexistence result

4.1. **Main result of this section.** Generalizing the notation from (13) and (15) let

$$\mathcal{C}_n := \{a_0X + a_1X^q + a_2X^{q^3} : a_0, a_1, a_2 \in \mathbb{F}_{q^n}\}. \tag{19}$$

As we have seen in Section 3 the MRD codes of $\mathbb{F}_q^{n\times n}$, $n \leq 9$, which are not equivalent to the generalized Gabidulin codes but have maximum left and right idealisers are, up to adjoint and Delsarte dual operations, equivalent either to $\mathcal{C}_7$ (for q odd) or to $\mathcal{C}_8$ (for $q \equiv 1 \pmod 3$). It is natural to ask whether the family $\mathcal{C}_n$ contains new MRD codes for larger values of n. In this direction, we will prove the following result.

Theorem 4.1. *For $n \geq 9$ and any prime power q, $\mathcal{C}_n$ is not an MRD code.*

To prove Theorem 4.1, we will need the following lemma.

Lemma 4.2. [26, Proposition 2] *Let F be a polynomial in $\mathbb{F}_q[X, Y]$ and suppose that F is not absolutely irreducible, that is, $F = AB$ where the coefficients of A and B are in the algebraic closure of $\mathbb{F}_q$. Let $P = (u, v)$ be a point in the affine plane* $\mathrm{AG}(2, q)$ *and write*

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots,$$

where F_i is zero or homogeneous of degree i and $F_m \neq 0$. Assume that F_m is completely reducible as a power of a linear polynomial and $gcd(F_m, F_{m+1}) = 1$. Then $I(P, \mathcal{A}\cap\mathcal{B}) = 0$, where $\mathcal{A}$ and $\mathcal{B}$ are the curves defined by A and B respectively.

Proof of Theorem 4.1. First, for $n = 9$, it is easy to see that $X^{q^3} - X \in \mathcal{C}_9$ has exactly q^3 roots which implies that $\mathcal{C}_9$ is not MRD. In the rest of the proof we will assume $n \geq 10$.

We will apply Theorem 2.6 with $\mathcal{S} = \{0, 1, 3\}$ and $\mathcal{T} = \{0, 1, 2\}$. It gives us that $\mathcal{C}_n$ is an MRD code if and only if $\mathcal{H} \setminus \mathcal{W}$ does not have $\mathbb{F}_{q^n}$-rational points, where $\mathcal{H}$ and $\mathcal{W}$ are projective curves defined by

$$H(X_0, X_1, X_2) := -X_0^{q^3}X_1^qX_2+X_0^qX_1^{q^3}X_2+X_0^{q^3}X_1X_2^q-X_0X_1^{q^3}X_2^q-X_0^qX_1X_2^{q^3}+X_0X_1^qX_2^{q^3}$$

and

$$W(X_0, X_1, X_2) := -X_0^{q^2}X_1^qX_2+X_0^qX_1^{q^2}X_2+X_0^{q^2}X_1X_2^q-X_0X_1^{q^2}X_2^q-X_0^qX_1X_2^{q^2}+X_0X_1^qX_2^{q^2},$$

respectively.

It is clear that $H(0, X_1, X_2) = W(0, X_1, X_2) = 0$. Hence, we only have to investigate the points $\langle (1, x, y) \rangle$ for x and $y \in \mathbb{F}_{q^n}$. By calculation,

$$H(1, X, Y) = (X^q - X^{q^3})(Y^q - Y) + (Y^{q^3} - Y^q)(X^q - X),$$

$$W(1, X, Y) = (X^q - X^{q^2})(Y^q - Y) + (Y^{q^2} - Y^q)(X^q - X).$$

Then to prove our assertion it is enough to show that the affine curve $\mathcal{V}$ defined by

$$V(X, Y) := \frac{H(1, X, Y)}{W(1, X, Y)} = \frac{(Y^q - Y)^{q^2-1} - (X^q - X)^{q^2-1}}{(Y^q - Y)^{q-1} - (X^q - X)^{q-1}} + 1 \tag{20}$$

admits at least one $\mathbb{F}_{q^n}$-rational point (x, y) which does not lie on the affine part of the curve $\mathcal{W}$ defined by $W(1, X, Y)$.

By calculation,

$$V(X, Y) = \prod_{\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} ((X^q - X) - \gamma(Y^q - Y)) + 1. \tag{21}$$

It is not difficult to get an upper bound for the number of affine points in $\mathcal{V} \cap \mathcal{W}$. If a point (x, y) is on $\mathcal{W}$, then it satisfies one of the following conditions:

(a) $x^q - x = 0$, i.e. $x \in \mathbb{F}_q$;
(b) $y^q - y = 0$, i.e. $y \in \mathbb{F}_q$;
(c) $x^q - x = \xi(y^q - y)$, where $\xi \in \mathbb{F}_q^*$.

When $x \in \mathbb{F}_q$, $V(x, y) = (y^q - y)^{q^2-q} + 1$. It follows that $(y^q - y)^{q^2} = -(y^q - y)^q$ and $y \notin \mathbb{F}_q$. Hence $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and there are exactly $q(q^2 - q) = q^3 - q^2$ points (x, y) of type (a) on $\mathcal{V} \cap \mathcal{W}$.

When $y \in \mathbb{F}_q$, by symmetry, we get another $q^3 - q^2$ points in $\mathcal{V} \cap \mathcal{W}$.

When $x^q - x = \xi(y^q - y)$ with $\xi \in \mathbb{F}_q^*$,

$$\begin{aligned} V(x, y) &= \prod_{\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} (\xi - \gamma)(y^q - y)^{q^2-q} + 1 \\ &= \frac{\prod_{\gamma \in \mathbb{F}_{q^2} \setminus \{\xi\}} (\xi - \gamma)}{\prod_{\gamma \in \mathbb{F}_q \setminus \{\xi\}} (\xi - \gamma)} (y^q - y)^{q^2-q} + 1 \\ &= (y^q - y)^{q^2-q} + 1. \end{aligned}$$

This means that $y \notin \mathbb{F}_q$ and y also satisfies

$$(y^q - y)^q = y - y^q.$$

Thus for given ξ, there are exactly $q^2 - q$ solutions of y and for each y, there are exactly q solutions of x for $x^q - x = \xi(y^q - y)$. As ξ can be taken any value in $\mathbb{F}_q^*$, there are in total $q^2(q-1)^2$ points (x, y) of type (c).

Therefore we have proved that there are $B_a := q^2(q-1)^2 + 2(q^3 - q^2) = q^4 - q^2$ affine points in $\mathcal{V} \cap \mathcal{W}$, hence the number of $\mathbb{F}_{q^n}$-rational affine points in $\mathcal{V} \cap \mathcal{W}$ is at most $q^4 - q^2$.

Let

$$V^*(X, Y, T) = \prod_{\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} ((X^q - XT^{q-1}) - \gamma(Y^q - YT^{q-1})) + T^{q^3 - q^2}$$

be the homogenized polynomial of V. By considering the zeros of

$$V^*(X,1,0) = \prod_{\gamma\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q}(X^q-\gamma) = \left(\prod_{\gamma\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q}(X-\gamma)\right)^q, \tag{22}$$

we see that the points at infinity of $\mathcal{V}$ are $R_\gamma = (\gamma,1,0)$ for $\gamma\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Hence there are q^2-q points at infinity.

Very recently, Giulietti, Korchmáros and Timpanella [21] also investigated this curve and they called it the Dickson-Guralnick-Zieve curve after the work [23] by Guralnick and Zieve, see also [4]. They can show that this curve is absolutely irreducible [21, Proposition 4.7] and the genus of $\mathcal{V}$ is $g_q = \frac{1}{2}q(q-1)(q^3-2q-2)+1$ [21, Theorem 4.10]. Moreover, by Lemmas 4.5 and 4.6 in [21], each singular point of $\mathcal{V}$ has a unique branch centered on it, which means the number R_{q^n} of the $\mathbb{F}_{q^n}$-places of the associated function field of $\mathcal{V}$ equals the number of $\mathbb{F}_{q^n}$-rational points of $\mathcal{V}$ (for further details see [24, Chapter 4]). By the Hasse-Weil Theorem, one gets

$$\#\mathcal{V}(\mathbb{F}_{q^n}) = R_{q^n} \geq q^n+1-2g_q\sqrt{q^n}.$$

Together with the total number B_a of the affine points in $\mathcal{V}\cap\mathcal{W}$ and the q^2-q points of $\mathcal{V}$ at infinity, the existence of an affine $\mathbb{F}_{q^n}$-point (x,y) on $\mathcal{V}\setminus\mathcal{W}$ is ensured whenever

$$q^n+1-2g_q\sqrt{q^n} > q^4-q^2+q^2-q = q^4-q. \tag{23}$$

By plugging the value of g_q into it, it is straightforward to check that (23) holds for $n\geq 10$.

In [21], the authors proved the absolutely irreducibility by analyzing the branches of the curve. In the rest of our proof, we present an alternative proof only using Bézout's theorem, see for example [24, Chapter 3]. We assume that $\mathcal{V}$ splits into two components $\mathcal{A}$ and $\mathcal{B}$ sharing no common irreducible component. Then we determine all possible singular points of $\mathcal{V}$ and show that the sum of all intersection numbers of $\mathcal{A}$ and $\mathcal{B}$ equals 0. Then by Bézout's theorem, we see that one of $\mathcal{A}$ and $\mathcal{B}$ must be a constant.

It appears quite complicated to compute the affine singular points (α,β) of $\mathcal{V}$ and the expansion of $V(X+\alpha,Y+\beta)$ directly. Instead, we investigate those for

$$U(X,Y) = -H(1,X,Y) = (X^{q^3}-X^q)(Y^q-Y)-(X^q-X)(Y^{q^3}-Y^q).$$

By (20), it is clear that

$$V(X,Y) = \frac{U(X,Y)}{S(X,Y)},$$

where $S(X,Y) = -W(1,X,Y)$. Hence every singular point of $\mathcal{V}$ is also a singular point of the curve $\mathcal{U}$ defined by U.

By calculation,

$$\frac{\partial U(X,Y)}{\partial X} = Y^{q^3}-Y^q, \qquad \frac{\partial U(X,Y)}{\partial Y} = -(X^{q^3}-X^q).$$

It follows that every affine singular point (x,y) of $\mathcal{U}$ belongs to $\mathbb{F}_{q^2}\times\mathbb{F}_{q^2}$.

When $\alpha, \beta \in \mathbb{F}_q$, by (21), (α, β) is not a point on $\mathcal{V}$. We only have to consider the points $(\alpha, \beta) \in \mathbb{F}_{q^2}^2 \setminus \mathbb{F}_q^2$. By calculation,

$$\begin{aligned}
&U(X+\alpha, Y+\beta)\\
=&(\beta^q-\beta)(X^{q^3}-X^q)-(\alpha^q-\alpha)(Y^{q^3}-Y^q)+U(X,Y)\\
=&(\beta-\beta^q)X^q-(\alpha-\alpha^q)Y^q+XY(X^{q-1}-Y^{q-1})+\cdots\\
=&(\bar{\beta}X-\bar{\alpha}Y)^q+XY(X^{q-1}-Y^{q-1})-XY(X^{q^2-1}-Y^{q^2-1})\\
&+(\bar{\alpha}Y-\bar{\beta}X)^{q^3}+(XY(X^{q^2-1}-Y^{q^2-1}))^q,
\end{aligned}$$

where $\bar{\beta}^q = \beta - \beta^q$ and $\bar{\alpha}^q = \alpha - \alpha^q$. As $(\alpha, \beta) \notin \mathbb{F}_q \times \mathbb{F}_q$, $\bar{\beta}X - \bar{\alpha}Y \neq 0$.

It is routine to compute that

$$\begin{aligned}
S(X+\alpha, Y+\beta) =&(\bar{\alpha}Y-\bar{\beta}X)+(\bar{\beta}X-\bar{\alpha}Y)^{q^2}+XY(X^{q-1}-Y^{q-1})\\
&+(XY(X^{q-1}-Y^{q-1}))^q+XY(X^{q^2-1}-Y^{q^2-1}).
\end{aligned}$$

As

$$\bar{\beta}^q = -\bar{\beta},\ \bar{\alpha}^q = -\bar{\alpha},$$

$\bar{\beta}X - \bar{\alpha}Y$ divides $XY(X^{q-1}-Y^{q-1})$ and $XY(X^{q^2-1}-Y^{q^2-1})$ for all $(\alpha, \beta) \in \mathbb{F}_{q^2}^2 \setminus \mathbb{F}_q^2$. Thus

$$U^*(X+\alpha, Y+\beta) = \frac{U(X+\alpha, Y+\beta)}{\bar{\beta}X - \bar{\alpha}Y}$$

and

$$S^*(X+\alpha, Y+\beta) = \frac{S(X+\alpha, Y+\beta)}{\bar{\beta}X - \bar{\alpha}Y}$$

are both polynomials.

Let $\mathcal{U}^*$ be the curve defined by the polynomial $U^*(X+\alpha, Y+\beta)$. Assume that $\mathcal{U}^*$ splits into two components $\mathcal{X}$ and $\mathcal{Y}$. It is clear that $\bar{\beta}X - \bar{\alpha}Y$ does not divide $\frac{XY(X^{q-1}-Y^{q-1})}{\bar{\beta}X-\bar{\alpha}Y}$ which is the term of the second lowest degree of $U^*(X+\alpha, Y+\beta)$. By Lemma 4.2, the intersection number $I((0,0), \mathcal{X} \cap \mathcal{Y})$ is zero.

As $U^*(X+\alpha, Y+\beta) = V(X+\alpha, Y+\beta)S^*(X+\alpha, Y+\beta)$, we also get

$$I((\alpha, \beta), \mathcal{A} \cap \mathcal{B}) \leq I((0,0), \mathcal{X} \cap \mathcal{Y}) = 0.$$

Next we investigate the singular points of $\mathcal{V}$ at infinity. By (22) the points of $\mathcal{V}$ at infinity are R_γ for $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. To determine the intersection number of $\mathcal{A}$ and $\mathcal{B}$ at each R_γ, we consider

$$\begin{aligned}
-H(Y, X+\gamma, 1)/Y =&(X^{q^3}+\gamma^q-(X^q+\gamma^q)Y^{q^3-q})(1-Y^{q-1})\\
&-(X^q+\gamma^q-(X+\gamma)Y^{q-1})(1-Y^{q^3-q})\\
=&(X^q-X+\gamma^q-\gamma)Y^{q^3-1}-X^{q^3}Y^{q-1}+X^{q^3}\\
&+XY^{q-1}-X^q+(\gamma-\gamma^q)Y^{q-1}.
\end{aligned}$$

As $(\gamma - \gamma^q)Y^{q-1}$ is the term of the lowest degree in it, each point R_γ is a non-ordinary singular point of $\mathcal{V}$ of multiplicity $q-1$. Note that $Y \nmid XY^{q-1} - X^q$. By Lemma 4.2, $I(R_\gamma, \mathcal{A} \cap \mathcal{B}) = 0$.

Denote the degrees of $\mathcal{A}$ and $\mathcal{B}$ by d_1 and d_2, respectively. By Bézout's theorem,

$$d_1 d_2 = \sum I(P, \mathcal{A} \cap \mathcal{B}).$$

According to our previous calculation, the right-hand side of it equals 0, whence one of d_1 and d_2 has to be 0. Therefore, $\mathcal{V}$ is absolutely irreducible and this completes the proof. □

4.2. **Further results and open problems.** We investigate further the curves of the previous part in order to show that $\mathcal{C}_n$ is an MRD code if and only if a certain rank-metric code of dimension $2n$ over $\mathbb{F}_q$ in $\mathbb{F}_q^{(n-1)\times n}$ is an MRD code. Assume that $H(1,X,Y)/W(1,X,Y) = 0$. By (20),

$$(Y^q - Y)^{q^2-1} + (Y^q - Y)^{q-1} = (X^q - X)^{q^2-1} + (X^q - X)^{q-1}.$$

If we set

$$\overline{X} = X^q - X \text{ and } \overline{Y} = Y^q - Y, \tag{24}$$

then it becomes

$$\overline{Y}^{q^2-1} + \overline{Y}^{q-1} = \overline{X}^{q^2-1} + \overline{X}^{q-1}. \tag{25}$$

Hence, $\mathcal{H}$ contains no $\mathbb{F}_{q^n}$-rational points besides those on $\mathcal{W}$ if and only if every $\mathbb{F}_{q^n}$-rational point $\langle(1,x,y)\rangle$ on the curve defined by the affine equation (25) satisfies $(x^q - x)^{q-1} = (y^q - y)^{q-1}$.

Assume that $\overline{Y}^{q^2-1} + \overline{Y}^{q-1} = \overline{X}^{q^2-1} + \overline{X}^{q-1} = -t$, for some $t \in \mathbb{F}_{q^n}$. It follows that $\overline{X}$ and $\overline{Y}$ are both roots of

$$Z^{q^2} + Z^q + tZ \in \mathbb{F}_{q^n}[Z]. \tag{26}$$

The polynomial (26) has at most q^2 roots. If (26) has q roots, then for any two non-zero roots, z_1 and z_2, it holds that $z_1^{q-1} = z_2^{q-1}$. This implies that the corresponding point $\langle(1,x,y)\rangle$ is on $\mathcal{W}$. If the polynomial (26) has q^2 roots, then there always exist two of them, z_1 and z_2, which are $\mathbb{F}_q$-linearly independent, or equivalently $z_1^{q-1} \neq z_2^{q-1}$. By (24) the roots of (26) have to be in $\{x \colon \mathrm{Tr}_{q^n/q}(x) = 0\}$. Hence, $z_1^{q-1} = z_2^{q-1}$ holds for any two roots z_1 and z_2 of (26) if and only if (26) has at most q roots in $\mathbb{F}_{q^n}$ with trace zero over $\mathbb{F}_q$.

Therefore, we have proved the following result.

Proposition 4.3. *The set of linearized polynomials $\mathcal{C}_n$ is an MRD code if and only if (26) has at most q roots in $\{y \in \mathbb{F}_{q^n} \colon \mathrm{Tr}_{q^n/q}(y) = 0\}$ for each $t \in \mathbb{F}_{q^n}$.*

Proposition 4.3 shows us that $\mathcal{C}_n$ is an MRD if and only if $\{aX + bX^q + bX^{q^2} \colon a, b \in \mathbb{F}_{q^n}\}$ with restriction to the $(n-1)$-dimensional $\mathbb{F}_q$-subspace $\{x \in \mathbb{F}_{q^n} \colon \mathrm{Tr}_{q^n/q}(x) = 0\}$ of $\mathbb{F}_{q^n}$ is an MRD code of size q^{2n} in $\mathbb{F}_q^{(n-1)\times n}$.

Besides the adjoint and Delsarte dual operations there is another operation which preserve the maximality of the idealisers of certain families of MRD codes and can be used to produce possibly new families:

Proposition 4.4. *Fix a prime power q and an integer n. The set*

$$\{a_0 X^{\sigma^{t_0}} + a_1 X^{\sigma^{t_1}} + \ldots + a_{k-1} X^{\sigma^{t_{k-1}}} \colon a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^{nm}}\} \tag{27}$$

with $\sigma = q^{ms}$, $\gcd(s,n) = 1$ is an $\mathbb{F}_{q^m}$-linear MRD code for every positive integer m if and only if

$$\{a_0 X^{\tau^{t_0}} + a_1 X^{\tau^{t_1}} + \ldots + a_{k-1} X^{\tau^{t_{k-1}}} \colon a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^{nm}}\} \tag{28}$$

with $\tau = q^{mt}$, $\gcd(t,n) = 1$ is an $\mathbb{F}_{q^m}$-linear MRD code for every positive integer m.

Proof. Suppose that the condition holds for the codes defined by (27). Let z denote the multiplicative inverse of s modulo n, let m and t be any positive integers with $\gcd(t,n)=1$. By our assumption

$$\{a_0X^{\sigma^{t_0}}+a_1X^{\sigma^{t_1}}+\ldots+a_{k-1}X^{\sigma^{t_{k-1}}}: a_0,a_1,\ldots,a_{k-1}\in\mathbb{F}_{q^{nztm}}\} \tag{29}$$

with $\sigma=q^{sztm}$, is an $\mathbb{F}_{q^{ztm}}$-linear MRD code. Equivalently, the elements of (29) have kernels of dimension at most $k-1$ over $\mathbb{F}_{q^{ztm}}$. Let U be the $\mathbb{F}_{q^{ztm}}$-subspace of the roots in $\mathbb{F}_{q^{nztm}}$ of $f(X):=a_0X^{\sigma^{t_0}}+a_1X^{\sigma^{t_1}}+\ldots+a_{k-1}X^{\sigma^{t_{k-1}}}$ for some $a_0,a_1,\ldots,a_{k-1}\in\mathbb{F}_{q^{nm}}$. The polynomial f is in (29), thus the dimension of U over $\mathbb{F}_{q^{ztm}}$ is at most $k-1$. The $\mathbb{F}_{q^m}$-subspace of the roots of f in the field $\mathbb{F}_{q^{nm}}$ is $U\cap\mathbb{F}_{q^{nm}}$. Since $\gcd(zt,n)=1$, according to [34, Lemma 3.1], the dimension over $\mathbb{F}_{q^m}$ of $U\cap\mathbb{F}_{q^{nm}}$ is at most $k-1$ and hence

$$\{a_0X^{\tau^{t_0}}+a_1X^{\tau^{t_1}}+\ldots+a_{k-1}X^{\tau^{t_{k-1}}}: a_0,a_1,\ldots,a_{k-1}\in\mathbb{F}_{q^{nm}}\}$$

with $\tau=q^{sztm}$ is an $\mathbb{F}_{q^m}$-linear MRD code. Since $sz\equiv 1 \pmod n$ this is the same code as the one defined in (28). □

Now, assume that the monomials $X^{\sigma^{t_0}},X^{\sigma^{t_1}},\ldots,X^{\sigma^{t_{k-1}}}$, where $\sigma=q^s$ and $\gcd(s,n)=1$, define an MRD code $\mathcal{C}_{\sigma,t_0,\ldots,t_{k-1}}$ over every extension $\mathbb{F}_{q^{mn}}$ of $\mathbb{F}_{q^n}$. Then Proposition 4.4 guarantees that $\mathcal{C}_{\tau,t_0,\ldots,t_{k-1}}$ is an MRD code over $\mathbb{F}_{q^{mn}}$ as well, with $\tau=q^t$ for any positive integer t such that $\gcd(t,n)=1$.

It is easy to see that for generalized Gabidulin codes and for $\mathcal{C}_7$ and $\mathcal{C}_8$, the condition in Proposition 4.4 holds. If we apply Proposition 4.4 to $\mathcal{C}_7$ or $\mathcal{C}_8$, the resulting codes can be obtained also via the adjoint operation.

Question 4.5. Is there any family of $n\times n$ MRD codes with maximum idealisers such that the condition in Proposition 4.4 does not hold?

To conclude our paper, we would like to present two open questions concerning the asymptotic behavior of MRD codes with maximum idealisers.

Question 4.6. Is it true that for any positive integer k, there exists a constant c, depending only on k, such that for $n>c$ the set of linearized polynomials

$$\left\{\sum_{i=0}^{k-1}a_ix^{q^{t_i}}: a_0,\ldots,a_{k-1}\in\mathbb{F}_{q^n}\right\}$$

is an MRD code only if $t_0,\ldots,t_{k-1}$ is an arithmetic progression of $\mathbb{Z}_n$?

If the answer to Question 4.6 is negative, then it is natural to ask the following, weaker question.

Question 4.7. Is it true that, for any k distinct positive integers $t_0,t_1,\ldots,t_{k-1}$ which do not form an arithmetic progression of $\mathbb{Z}$, there exists a constant c such that for $n>c$ the set of linearized polynomials

$$\left\{\sum_{i=0}^{k-1}a_ix^{q^{t_i}}: a_0,\ldots,a_{k-1}\in\mathbb{F}_{q^n}\right\}$$

is not MRD?

Remark 2. Recently, in [3] Bartoli, jointly with the fourth author of the paper, analyzed Questions 4.6 and 4.7. In particular, they provide an affirmative answer to Question 4.7 for $q>5$, and a partial result for $q=2,3,4$ and 5. These results also yield classification of some special type of linear sets in [41].

References

[1] D. Bartoli, C. Zanella and F. Zullo. A new family of maximum scattered linear sets in $\mathrm{PG}(1, q^6)$. *arXiv:1910.02278 [math]* Oct. 2019.

[2] D. Bartoli and Y. Zhou. Exceptional scattered polynomials. *Journal of Algebra*, 509(1): 507-534, 2018.

[3] D. Bartoli and Y. Zhou. Asymptotics of Moore exponent sets. *arXiv:1907.11100 [math]*, July 2019.

[4] H. Borges. On multi-frobenius non-classical plane curves. *Archiv der Mathematik*, 93(6): 541–553,2009.

[5] A. Cossidente, G. Marino, and F. Pavese. Non-linear maximum rank distance codes. *Designs, Codes and Cryptography*, 79(3):597–609, 2016.

[6] B. Csajbók, G. Marino, and O. Polverino. Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$. *J. Combin. Theory Ser. A*, 157:402–426, 2018.

[7] B. Csajbók, G. Marino, O. Polverino, and C. Zanella. A new family of MRD-codes. *Linear Algebra Appl.*, 548:203–220, 2018.

[8] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Maximum scattered linear sets and MRD-codes. *J. Algebraic Combin.*, 46:1–15, 2017.

[9] B. Csajbók, G. Marino, and F. Zullo. New maximum scattered linear sets of the projective line. *Finite Fields and their Applications* 54:133–150, 2017.

[10] B. Csajbók and C. Zanella. On the equivalence of linear sets. *Designs, Codes and Cryptography*, 81(2):269–281, 2016.

[11] B. Csajbók and C. Zanella. On scattered linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$. *Finite Fields Appl.*, 41:34–54, 2016.

[12] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems. Algebraic structures of MRD codes. *Advances in Mathematics of Communications*, 10(3):499–510, 2016.

[13] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, Nov. 1978.

[14] U. Dempwolff and Y. Edel. Dimensional dual hyperovals and APN functions with translation groups. *Journal of Algebraic Combinatorics*, 39(2):457–496, June 2014.

[15] U. Dempwolff and W. M. Kantor. Orthogonal dual hyperovals, symplectic spreads, and orthogonal spreads. *Journal of Algebraic Combinatorics*, 41(1):83–108, May 2015.

[16] G. Donati and N. Durante. A generalization of the normal rational curve in $\mathrm{PG}(d, q^n)$ and its associated non-linear MRD codes. *Designs, Codes and Cryptography*, 86(6):1175–1184, 2018.

[17] N. Durante and A. Siciliano. Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries. *The Electronic Journal of Combinatorics*, 24:P2.33, 2017.

[18] E.M. Gabidulin. Theory of codes with maximum rank distance. *Problems of information transmission*, 21:3–16, 1985.

[19] E.M. Gabidulin. Public-key cryptosystems based on linear codes over large alphabets: efficiency and weakness. In *Codes and Cyphers*, pages 17–31. Formara Limited, 1995.

[20] M. Gadouleau and Z. Yan. Properties of codes with the rank metric. In *IEEE Global Telecommunications Conference 2006*, pages 1–5, 2006.

[21] M. Giulietti, G. Korchmáros and M. Timpanella On the Dickson-Guralnick-Zieve curve. *Journal of Number Theory* 196:114–138, 2018.

[22] R. Gow, R. Quinlan. Galois extensions and subspaces of alternating bilinear forms with special rank properties. *Linear Algebra Appl.*, 430:2212–2224, 2009.

[23] R.M. Guralnick and M.E. Zieve. Work on Automorphisms of Ordinary Curves. *in preparation* (Talk in Leiden, Workshop on Automorphism of Curves, 18-08-2004).

[24] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres. Algebraic Curves over a Finite Field. *Princeton Series in Applied Mathematics*, Princeton (2008).

[25] A.-L. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank metric code constructions. *Advances in Mathematics of Communications.*, 11(3): 533-548, 2017.

[26] H. Janwa, G. McGuire, and R. Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$. *Journal of Algebra*, 178(2):665–676, Dec. 1995.

[27] N.L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[28] R. Koetter and F. Kschischang. Coding for errors and erasure in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.

[29] A. Kshevetskiy and E. Gabidulin. The new construction of rank codes. In *International Symposium on Information Theory, 2005. ISIT 2005. Proceedings*, pages 2105–2108, Sept. 2005.

[30] M. Lavrauw and O. Polverino. Finite semifields. In L. Storme and J. De Beule, editors, *Current research topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, 2011.

[31] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[32] D. Liebhold and G. Nebe. Automorphism groups of Gabidulin-like codes. *Archiv der Mathematik*, 107(4):355–366, Oct. 2016.

[33] G. Lunardon. MRD-codes and linear sets. *Journal of Combinatorial Theory, Series A*, 149:1–20, July 2017.

[34] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A*, 159:79-106, Oct. 2018.

[35] G. Lunardon, R. Trombetti, and Y. Zhou. On kernels and nuclei of rank metric codes. *Journal of Algebraic Combinatorics*, 46(2):313–340, Sept. 2017.

[36] P. Lusina, E. Gabidulin, and M. Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, Oct. 2003.

[37] M. Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arith.*, 132 (2008), no. 4, 329-–350.

[38] G. Marino, M. Montanucci, and F. Zullo. MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$, *Linear Algebra Appl.* 591 (2020), 99–114.

[39] E.H. Moore. A two-fold generalization of Fermat's theorem. *Bull. Amer. Math. Soc.*, 2(7):189–199, 1896.

[40] K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. *IEEE Transactions on Information Theory*, 60(11):7035–7046, 2014.

[41] V. Napolitano, O. Polverino, G. Zini and F. Zullo. Linear sets from projection of Desarguesian spreads *arXiv:2001.08685 [math]*, Jan. 2020.

[42] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[43] K. Otal and F. Özbudak. Additive rank metric codes. *IEEE Transactions on Information Theory*, 63(1):164–168, Jan. 2017.

[44] K. Otal and F. Özbudak. Some new non-additive maximum rank distance codes. *Finite Fields and Their Applications*, 50:293–303, Mar. 2018.

[45] A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, 80(1):197–216, 2016.

[46] R.M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, Mar 1991.

[47] K.-U. Schmidt and Y. Zhou. On the number of inequivalent Gabidulin codes. *Designs, Codes and Cryptography*, 86(9):1973–1982, 2018.

[48] J. Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10(3):475–488, 2016.

[49] J. Sheekey. New Semifields and new MRD Codes from Skew Polynomial Rings. *J. Lond. Math. Soc. (2)* (2019), 1–25.

[50] J. Sheekey, and G. Van de Voorde. Rank-metric codes, linear sets and their duality. *Des. Codes Cryptogr.* 88 (2020), 655–675.

[51] H. Taniguchi and S. Yoshiara. A unified description of four simply connected dimensional dual hyperovals. *European Journal of Combinatorics*, 36:143–150, 2014.

[52] R. Trombetti and Y. Zhou. A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$. *IEEE Transaction on Information Theory*, 65(2):1054–1062, 2019.

[53] B. Wu and Z. Liu. Linearized polynomials revisited. *Finite Fields and Their Applications*, 22:79–100, 2013.
[54] C. Zanella, and F. Zullo. Vertex properties of maximum scattered linear sets of PG$(1, q^n)$. *Discrete Math.* 343(5) (2020).

[1]MTA–ELTE Geometric and Algebraic Combinatorics Research Group, ELTE Eötvös Loránd University, Budapest, Hungary, Department of Geometry, 1117 Budapest, Pázmány P. stny. 1/C, Hungary
Email address: csajbokb@cs.elte.hu

[2]Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli "Federico II", Via Cintia, Monte S.Angelo I-80126 Napoli, Italy
Email address: giuseppe.marino@unina.it

[3]Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Viale Lincoln 5, I- 81100 Caserta, Italy
Email address: olga.polverino@unicampania.it

[4]College of Liberal Arts and Sciences, National University of Defense Technology, 410073 Changsha, China
Email address: yue.zhou.ovgu@gmail.com